Appendix 3 to
Tenth Amendment of
Master Services Agreement

Exhibit 2.8.1
Statement of Work
Security Monitoring and Device Management Services

DIR-MSS-SCP-001

January 15, 2021

Exhibit to Managed Security Services Service Component Provider Master Services Agreement

DIR Contract No. DIR-MSS-SCP-001

Between

The State of Texas, acting by and through
the Texas Department of Information Resources

and

AT&T Corp.

Exhibit 2.8.1

Statement of Work

Security Monitoring and Device Management Services

January 15, 2021

Change Log			
CCR/CN	Amendment	Date	Description
CCR-00314	Amendment 1	09/19/2018	• Updated RU definition for SOC Monitoring and Alerting Requirements in Section 3.1.9.1 • Cosmetic updates (e.g., footer, revision number, etc.)
CCR-000329	Amendment 2	12/12/2018	• Adding High Availability Platinum Services.
CCR-000381	Amendment 5	03/19/2020	• Added SOC Monitoring and Alerting Requirements (24x7) in Section 3.1.9.2
CCR-000437	Amendment 8	10/23/2020	• Section 3.1: Adds Endpoint Detection and Response (EDR) Services. • Section 3.1.2: Adds language to reflect addition of Endpoint Detection and Response (EDR) Services.
CCR-000444	Amendment 9	12/18/2020	• Added SOC Monitoring and Alerting Requirements Remote (24x7) in Section 3.1.10.2
CCR-000XXX	Amendment 10	1/15/2021	• Updated list of Service Areas in Section 3.1 • Added Advanced Threat Hunting in Section 3.1.11 • Added clarifying language in Sections 3.1 and 3.1.10

Table of Contents

1.0 Managed Security Services – Security Monitoring and Device Management

1.1 Services Overview

This **Exhibit 2.8.3 -** Managed Security Services – Security Monitoring and Device Management sets forth the roles and responsibilities of the Parties for the Services provided under the Agreement.

DIR is seeking a Service Provider to deliver Security Monitoring and Device Management (MDM) Services to assist Customers in meeting internal needs, as well as any state and Federal legal and regulatory requirements for providing effective protection of their networks and computing platforms.

The type and scope of work will be determined by the Customer and agreed between the Service Provider and Customer.

1.2 Service Strategies and Objectives

Managed Security Services (MSS) is a procurement and service delivery mechanism to be offered by Texas DIR for customers to engage a provider to obtain governed security Services. Customers may request specific solution proposals that assume the responsibilities defined in this Statement of Work that will be applied to a specific scope of work. The service level requirements are described and documented in **Exhibit 3** and its attachments; pricing is described and documented in **Exhibit 4** and its attachments.

2.0 Service Environment

2.1 Scope of the Infrastructure to Be Supported

The following sub-sections and related Appendices further describe and scope the Services to be supported and/or with which Service Provider shall comply. The Service Environment will be specifically defined at the time the Service Provider is engaged by a Customer to propose or deliver Services.

To provide general context across potential Service Environments, the following sections may reference general lists, descriptions or guidance to be considered by the Service Provider in responding to the DIR RFO.

2.1.1 Services and Data

1. All support Services must be situated and all agency-related data must reside within the contiguous United States at all times. DIR will not consider any support Services situated outside the United States nor will DIR allow any DIR Data to be stored outside the contiguous United States
2. All data or other information generated as a result of Services provided by any Service Component Provider must be protected and shared only with relevant stakeholders and may not be shared for the purposes of additional sales opportunities. All data must be protected in accordance with the Master Services Agreement (MSA).

2.1.2 Service Hours and Locations

All Services listed below must be offered based on the following service hour options:

1. 24x7x365: all Services to be provided 24 hours a day, 7 days a week, all 365 days per year.
2. 7am-7pm weekdays: all Services to be provided from 7am to 7pm weekdays, with on-call resource support provided during off hours.
3. DIR's preference is that all non-SOC Services, at a minimum, will be provided remotely.

Service Provider must provide Services at Customer locations, if a Customer requests such Services through the Request Management system, in accordance with the Service Management Manual. These Customer Requests will be priced at time of request based on the criteria defined in **Exhibit 4**, Pricing.

No off-shoring of resources or Services is allowed.

Reference **Attachment 4-A**, Service Provider Pricing Forms, for resource unit pricing models for the Services required in this Statement of Work.

2.1.3 Personnel

Service Provider will be responsible for providing appropriately skilled staffing to meet the Roles and Responsibilities and service levels set forth in this SOW.

NOTE: Customers may request, through the Request Management process, dedicated resources to provide Services at the Customer's location. Service Provider shall provide dedicated, onsite resources to support Customer's needs in accordance with the Service Management Manual. These Customer Requests will be priced at time of request based on the criteria defined in **Exhibit 4**, Pricing.

2.1.4 Policies, Procedures and Standards

The general policies, procedures and standards with which Services will comply are provided in **Attachment 6-B** Service Management Manual. Additional requirements will be determined if the Service Provider is engaged by a Customer to propose or deliver Services.

2.1.5 Network Connectivity

Service Provider is responsible for providing the necessary network connectivity to DIR Facilities required to support the Services in accordance with the established Service Levels.

2.1.6 Dashboard

Service Provider shall provide a dashboard for use by DIR and each Customer as defined in **Exhibit 2.1.2**, Cross-Functional Services. The dashboard shall provide a real-time user interface, showing a graphical presentation of the current status and historical trends of DIR's, the Customer's, or computer appliances' key performance indicators necessary to enable instantaneous and informed decisions to be made at a glance.

Customers will require a single tenant dashboard. However, DIR will require a multi-tenant dashboard allowing DIR to access the dashboard for any of the Customers.

2.1.7 Centralized Data Repository

Service Provider shall provide an on-line and secure Centralized Data Repository to store, at a minimum, all DIR Data, log files, and documentation generated as part of and required to perform the Services. All DIR Data shall be kept in accordance with the Customer's applicable record retention requirements. The Centralized Data Repository shall be single tenant for each Customer. DIR requires a multi-tenant Centralized Data Repository allowing access to the repository for other Customers. Service Provider is responsible per **Exhibit 2.1.2**, Cross-Functional Services, and **Exhibit 13**, Reports, to provide timely and integrated data feeds to the MSI for reports placed on the DCS Portal, including Configuration Management.

2.1.8 Systems and Tools

Service Provider is required to provide any tools (both hardware and software) necessary for the execution of the Services. Service Provider shall maintain tools to meet performance standards, processes and policies requirements, to maximize efficiency, and to minimize outages, as necessary.

Customers may request, through the Request Management process, that the Service Provider use the Customer's tools to provide the Services. These Customer Requests will be priced at time of request based on the criteria defined in **Exhibit 4**, Pricing.

Service Provider shall use the systems and tools provided by the MSI in delivering Services.

2.1.9 Operational Support

Service Provider is responsible for managing the technical operations that support the delivery of the Services according to best practices, including regular backups, capacity management, availability management, and Service Provider's own disaster recovery and business continuity. Operational support must be provided for any systems, Services, or components on a 24x7x365 basis, in accordance with DIR published processes in the Service Management Manual, including but not limited to maintaining current Hardware and Software version levels on all Systems, Services, and Components in compliance with 1 TAC 202, Customer published standards and processes, and DIR governance board. Reference **Exhibit 4-B** for hardware and software version requirements.

2.1.10 Transition Status Meetings

As directed by DIR, Status meetings will be held at DIR offices to update progress made, seek input from DIR, and to ensure that work is proceeding in the desired direction. Any issues affecting this project shall be addressed at these meetings. Initially, it is intended that these meetings will be held at least weekly. The frequency of these meetings may be altered to fit the then current need. At a minimum, the Status Meetings shall include:

1. Agenda – Service Provider shall provide a written agenda to DIR Project Manager at least 24 hours prior to meeting. This will allow DIR Project Manager the opportunity to include any additional topics.

2. Minutes - Service Provider shall keep minutes of each meeting and provide a written copy to DIR Project Manager within two (2) business days of the meeting. As a minimum, minutes shall address topics discussed, issues raised, and intended resolution of those issues.

3. Status Reports - Service Provider shall provide weekly written status reports to the DIR Project Manager. The written status reports shall address Tasks Completed, Tasks in Progress, Work to be Initiated During the Next Period, identified Risks with Risk Management approach, and Issues Requiring Management Attention. Issues Requiring Management Attention shall include, but not be limited to, any problems that may delay performance along with proposed corrective action, any failure of Service Provider or DIR to perform, any delay of Service Provider or DIR in performing, and any inadequacy in the performance of Service Provider or DIR.

In the event the Service Provider fails to timely specify in writing, within the applicable weekly reporting period, an Issue Requiring Management Attention for the Weekly Status Report, Service Provider shall not be entitled to rely upon such Issue as a purported justification for either (1) claiming Service Provider is entitled to receive any amount (including, without limitation, damages or additional charges arising out of a breach by DIR or Customer of a DIR or Customer obligation) with respect to Service Provider's obligations hereunder in excess of those previously agreed to; (2) failing to complete any of Service Provider's obligations hereunder or (3) requesting any reduction in or avoidance of damages or penalties. Submission of the above referenced status reports shall not alter, amend or modify Service Provider's or DIR's rights or obligations pursuant to any provision of the Contract.

2.1.11 Key Service Provider Personnel

Service Provider shall designate Key Personnel for the Service Component and each of the service areas in accordance with the MSA, **Section 8.1**, Key Service Provider Personnel. At a minimum, Key personnel shall include:

- Account Manager
- Executive Sponsor
- Transition Manager (TM)
- Technical Subject Matter Experts or Leads

All proposed personnel shall be immediately available to provide services as required. Key Service Provider Personnel may not be removed from the project without DIR's written permission.

2.1.12 Confidentiality

In providing Services under this contract, the Service Provider will have access to confidential information related to each Customer. Therefore, Service Provider may be required to execute a non-disclosure/confidentiality agreement with each Customer.

Information obtained by Service Provider in the performance of this Contract shall be used only for the purposes of carrying out the provisions of this Contract. Inspection by or disclosure of any such information to anyone other than an officer or employee of Service Provider or Customer, other than for the purposes of carrying out, and in accordance with, the provisions of this Contract, shall require prior written approval of the Customer.

Service Provider shall implement and document a comprehensive information security program. Service Provider shall use, implement, and document reasonable and appropriate security practices to make information secure. If the security of any shared data is compromised or breached by Service Provider, subcontractors, or third-parties, Service Provider shall notify DIR and Customer immediately, but no later than 12 hours after discovery of the potential compromise or breach. Service Provider shall be liable to Customer for any compromise or breach whatsoever and shall be liable for all reasonable and appropriate costs (as determined by DIR or the Customer) associated with remediating the compromise or breach, as defined in the Master Services Agreement.

2.1.13 Background Checks

Prior to commencement of any Services, Service Provider is required to conduct background and/or criminal history investigation of the Service Provider’s employees and subcontractors who will be providing Services under the resulting contract in accordance with MSA, **Section 8.6(g)**, Background and/or Criminal History Investigations, and **Exhibit 17**, Safety and Security.

2.1.14 Disaster Recovery

The Service Provider shall restore its operations in the event of any disaster that disrupts the Service Provider’s ability to deliver its Services. Customers may optionally request disaster recovery test support.

Disaster Recovery requirements for Service Provider are listed below:

1. Service Provider shall be responsible for providing the resources, including network connectivity to disaster location facilities, needed to support its disaster recovery strategy.
2. Service Provider shall develop, maintain, and implement comprehensive Disaster Recovery Plans necessary to support its Services.
3. Service Provider shall provide its Disaster Recovery Plan, with Architecture diagram, to DIR for review and approval. Disaster Recovery Plans and architecture diagrams will be submitted and reviewed at least once per fiscal year, unless additional reviews are requested by DIR or to resolve corrective actions identified in DR testing or through actual DR events.
4. Service Provider shall work with DIR, MSI, and the Customer to establish DR declaration procedures and documentation of those procedures, as appropriate.
5. Service Provider shall perform DR Services to meet or exceed the applicable Service Levels for each Service.
6. Service Provider shall recover its operations in the event of a disaster.
7. For Customer owned equipment, the Service Provider is responsible to restore the existing configurations onto the Customer provided device.
8. For Service Provider owned equipment, the Service Provider is responsible to restore Services based on the agreed upon processes and procedures. Upon declaration of a disaster, the Service Provider will submit a Disaster Recovery declaration fee to include labor and any supplemental costs outside of insurance costs to replace equipment as per **Exhibit 24**, Insurance and Risk of Loss, to restore normal operations.

2.1.15 Disaster Recovery Testing

The Service Provider shall coordinate with Customers and participate in Customer scheduled DR tests, as appropriate and necessary, in alignment with **Attachment 4-A**, Service Provider Pricing Form (MSS).

Service Provider shall work with Customers to ensure that Customer Disaster Recovery Tests are supported:

1. The Service Provider shall schedule and perform Disaster Recovery (DR) Testing and participate in scheduled DR Tests.
2. Service Provider shall conduct all testing activities in such a manner so that impacts to active production, test, and development environments are minimized. If an active environment is required to execute the test, the use of the environment must be communicated and approved by DIR and the Customer in writing prior to the test.
3. Service Provider shall notify DIR and Customers of any anticipated DR risks to the Service being provided.
4. Service Provider shall evaluate the results of the test and identify potential corrective actions.
5. Service Provider shall implement and track corrective actions until resolved.

3.0 Descriptions – Security Monitoring and Device Management

3.1 Security Monitoring and Device Management Service Component

Security Monitoring and Device Management Services (MDM) assist Customers in meeting internal needs, as well as any state and Federal legal and regulatory requirements for providing effective protection of their networks, devices, and computing platforms. MDM also entails identifying or otherwise discovering and analyzing security threats to the Customer's IT environment through such means as log monitoring, event monitoring and other device monitoring.

MDM includes the installation, configuration, and management of Service Provider equipment. MDM integrates log monitoring and analysis with threat analysis. The Security Monitoring and Device Management Service Provider (MDM SP) must be able to integrate with the Customer's current security and host logging capabilities to ensure that MDM Service Provider receives accurate and timely logs. Customers may require the MDM Service Provider provide a Security Information and Event Management solution for event correlation. Using the Customer's log information, an understanding of the Customer's infrastructure, and the MDM Service Provider's threat intelligence, the MDM Service Provider shall tailor threat notifications to the Customer's infrastructure and risk profile.

The MDM Service Provider shall bring expert level resources to ensure that equipment is efficiently and proficiently managed.

In addition to the above-described scope, the MDM Service Component includes but is not limited to the following Service Areas:

1. Endpoint Device Management
2. Endpoint Detection and Response (EDR) Services
3. Intrusion Detection Systems / Intrusion Prevention Systems
4. Host-Based Intrusion Prevention Systems
5. Managed Firewalls
6. Web Application Firewalls
7. Security Information and Event Management

8. Targeted Threat Research
9. MDS Service Requirements
10. Security Operations Center Services
11. Advanced Threat Hunting

3.1.1 Endpoint Device Management

The MDM Service Provider shall monitor and manage Customer endpoint devices, including, but not limited to desktop, laptop, and tablet computers for evidence of threats, indicators of compromise, and malware, providing alerts when an endpoint device may be compromised or malware is detected.

3.1.1.1 Endpoint Device Management Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following Endpoint Management service requirements:

1. MDM Service Provider's Endpoint Management solution shall process automatic detection and policy actions to bring devices into compliance if any or all tracked compliance components, as specified by the Customer, are missing.
2. Provide the ability to throttle the host's CPU utilization during scanning so that scanning is non-impacting to production systems and applications.
3. Conduct scans as directed by Customer (e.g., during non-business hours).
4. MDM Service Provider's Endpoint Management solution shall be able to integrate and export data and custom attributes into Customer's selected format.
5. Install, update, upgrade, patch, operate, and maintain Malware protection software and systems in accordance with Customer's security requirements for Software and Equipment in the Customer Environment as per agreement with the Customer, including all supported operating systems and platforms.
6. Update antivirus components on Customer devices as per agreement with the Customer and work with appropriate third-party vendors to immediately resolve any identified issues.
7. Perform real-time Malware protection scanning in accordance with Customer's security requirements.
8. Provide a web portal allowing remote execution by MDM Service Provider of multiple antivirus engines on Customer assets and deliver scan results back to the Centralized Data Repository.
   a. The Centralized Data Repository shall contain all relevant information regarding all scan results. The Customer and the MDM Service Provider will mutually determine the information to be retained. At a minimum, this information shall include:
      1. Date of scan;
      2. System(s)/equipment scanned;
      3. Antivirus engine(s) used to perform the scan;
      4. Results of the scan including any specific malware(s) or virus(es) detected;
      5. Systems or equipment affected and to the greatest extent possible, the location of the malware/virus.

9. Upon detection of a Malware infection, immediately, as defined by the applicable Security Incident Severity Level, notify and respond to Malware infections as directed by Customer policy. Response actions shall include, but are not necessarily limited to:
    a. Reverse engineer Malware to determine the following:
        1. Function of Malware
        2. Infection vector of the Malware
    b. Determine what, if any, data was/is leaked and the sensitivity of the data[1].
    c. Submit new Malware (zero-day) binaries to the Customer's designated antivirus vendor for inclusion in the next pattern release.
    d. Submit malicious URLs (Uniform Resource Locators) to the Customer's designated Web security vendor to be classified as malicious.
    e. Track Malware incident for reporting to the Customer.
    f. Update the Centralized Data Repository appropriately.
10. Provide the ability to re-route traffic from a Customer Service Location back to a central location and run the traffic through real-time Malware monitoring tools.
11. Eradicate Malware through techniques such as reverse engineering, custom scripting in endpoint management system, and working with the antivirus vendor.
12. Monitor antivirus logs to detect secondary Malware infections.
13. Monitor logs from web filtering, firewall, antivirus and proactive Malware tools for secondary Malware infections and possible zero-day infections.
14. Manage the validation scanning and application configuration to remove any false positives.
15. If required by the Customer, MDM Service Provider shall provide a means to capture any endpoint data that may be later required for a forensic investigation to be performed by the Incident Response (IR) Service Provider. MDM Service Provider shall provide such captured data to the IR Service Provider as required.
16. Participate in security incident response to provide additional security information the Customer may need to respond to or manage the incident until the threat is mitigated or resolved.
17. Provide two levels of service options, Platinum and Gold, for Customers to select based on availability and mean time to repair service levels defined in Attachment 3-A and Attachment 3-B. Platinum service requires high availability through a redundant failover environment – the failover environment must provide standby device(s) to support the primary device(s) in the event of device failure.

3.1.2 Endpoint Detection and Response (EDR) Services

The MDM Service Provider shall provide an autonomous solution for endpoint devices including Windows, Mac, and Linux systems. The autonomous solution will manage, detect, and respond

[1] Reference Data Classification Guide at: http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Data%20Classification%20Guide.docx

to provide near real time threat monitoring and response to threats and suspicious events including, but not limited to, malware and ransomware.

3.1.2.1 Endpoint Detection and Response (EDR) Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following Endpoint Detection Response service requirements:

1. The MDM Service Provider's Endpoint Detection and Response solution shall process automatic detection and policy actions against Customer's assets in accordance with Customer's predefined security policy. If any tracked compliance components, as specified by the Customer's order, are missing the Service Provider will bring those devices and policies into compliance.
2. MDM Service Provider's Endpoint Management solution shall be able to integrate and export data and custom attributes into Customer's selected standardized format.
3. Install, update, upgrade, patch, operate, and maintain agent software and systems in accordance with Customer's security requirements for Software and Equipment in the Customer Environment as per agreement with the Customer, including all supported operating systems and platforms.
4. Operating System Coverage (Windows, Linux, Mac, Cloud Workloads, Legacy Systems)
5. Threat detection:
    a. Provide the ability to detect malicious activity and anomalies on endpoints beyond just looking for file-based malware in accordance with Customer's security policy/requirements utilizing some of the following:
        1. On-devices Static Artificial Intelligence (AI)
        2. On-devices Behavior AI
        3. Detection of Exploits and Malicious Scripts
        4. Lateral Movement
    b. Conduct scans as directed by Customer in compliance with the customer's security policy (e.g., during non-business hours).
    c. Manage the validation scanning and application configuration to remove any false positives identified in reviews with Customer.
    d. Upon detection of a Malware infection, immediately, as defined by the applicable Security Incident Severity Level, notify and respond to Malware infections as directed by Customer policy.
6. Security incident containment:
    a. Response actions shall include any or the following, but are not necessarily limited to:
        1. Block security incidents at network endpoints to prevent attacks from spreading across the entire network.
        2. Provide any information available on any potential data was/is leaked/lost to be used by the Customer's Incident Response Team.
        3. Submit new Malware (zero-day) binaries to the Customer's designated antivirus vendor for inclusion in the next pattern release.
7. Incident response
    a. Provide security incidents prioritization report to help Customer's security teams respond to attacks faster.

b. Eradicate Malware through techniques such as reverse engineering, custom scripting in endpoint management system, and working with the antivirus vendor.
c. Re-route traffic from a Customer Service Location back to a central location and run the traffic through real-time Malware monitoring tools if Customer's security policies allow.
d. Apply predefined automation based on Customer's security policy.
e. Perform technology driven Remediation and Rollback.
f. Update the Centralized Data Repository appropriately.

8. Incident investigation:
   a. Have a Central Data Repository built to house all Customer's EDR data and prepare it for analysis.
   b. Provide a web portal allowing remote execution by MDM Service Provider on Customer assets and deliver scan results back to the Centralized Data Repository.
   c. The Centralized Data Repository shall contain all relevant information regarding all scan results. The Customer and the MDM Service Provider will mutually determine the information to be retained. At a minimum, this information shall include:

      1. Date of scan;
      2. System(s)/equipment scanned;
      3. Engine(s) used to perform the scan;
      4. Results of the scan including any items detected;
      5. Systems or equipment affected and to the greatest extent possible, the location of the malware/virus.

   d. If required by the Customer, MDM Service Provider shall provide a means to capture any endpoint data that may be later required for a forensic investigation to be performed by the Customer's Incident Response team(s). MDM Service Provider shall provide such captured data to the Customer as required.
   e. Participation in a security incident response by providing additional security information the Customer may need to respond to or manage the incident until the Customer declares the incident resolved.
9. Provide Platinum level only support based on availability and mean time to repair service levels defined in Attachment 3-A and Attachment 3-B.

3.1.3 Intrusion Detection Services / Intrusion Prevention Services (IDS/IPS)

The MDM Service Provider shall meet or exceed the following IDS/IPS requirements. MDM Service Provider shall offer Services for configuration, monitoring, change management, and support of the Customer's Intrusion Detection System (IDS) and Intrusion Preventions System (IPS). IDS/IPS Services shall include hardware and software owned by the Customer, third-party, and/or MDM Service Provider. The platform will analyze events for signs of possible security events/incidents, including, but not limited to, violations or imminent threats of violation of computer security policies, acceptable-use policies, malware propagation or security best practices. This Service shall include automated responses to detected security events/incidents, including, but not limited to, dropping packets, resetting connections, generating alerts, or quarantining intruders.

3.1.3.1 IDS / IPS Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following IDS/IPS service requirements:

1. Install, update, upgrade, patch, operate, manage, license (as appropriate), administer, and maintain network intrusion detection and prevention systems for all networks specified by Customer, using existing HIPS or MDM Service Provider proposed IPS devices, in accordance with Customer's security requirements for all Software and Equipment in the Customer Environment. Requirement includes upgrades, patches or fixes as needed to Hardware, Software, and firmware to ensure optimal performance and capacity of the Service
2. Configure the network-based IDS and IPS so as to comply with Customer's security requirements in order to identify, monitor, and potentially block suspicious patterns that may indicate abnormal activity or intrusion attempts. MDM Service Provider shall notify the Customer of high risk events as applicable.
3. Continuously tune configurations to maximize firewall capabilities and protections.
4. Monitor the Customer Networks for external intrusions and cyber-attacks and alert the appropriate Customer personnel so that countermeasures may be taken.
5. Perform ongoing tuning of the network IDS and IPS, system signatures, and configuration settings to minimize invalid alerts (i.e., false positives, alert volume, incorrectly blocked traffic, nuisance alerts, etc.). Such tuning must be authorized by Customer and documented by the MDM Service Provider as required by the Customer.
6. Upgrade the network IDS and IPS and all associated rules, signatures, settings and software when upgrades are: provided by the applicable manufacturer; when such upgrades are in accordance with industry best practices; or, as required to maintain compliance with Customer's security requirements.
7. Retain all collected data and logs in accordance with the Customer's applicable data retention requirements.
   a. The minimum data and log retention period for this service shall be 30 calendar days for both online and archive storage and shall be included in the MDM Service Provider's pricing for this service.
   b. Customers requesting to obtain additional storage may purchase that storage from the MDM Service Provider as a pass-through expense as defined in **Exhibit 4**, Pricing and Financial Revisions, Section 10, Pass-Through Expenses.
8. Respond to and confirm any suspected high events and make recommendations on whether traffic is malicious or legitimate and whether or not mitigations should be put into effect while working with the Customer's ISP DDOS monitoring service.
9. Participate in security incident response to provide additional security information the Customer may need to respond to or manage the incident until the threat is mitigated or resolved.
10. Manage, update, and add filters, or blocks, to control unauthorized data sources.
11. Provide recommendations to DIR and Customers on new IPS filters or blocks.
12. Manage automated data exchange capabilities between the IPS Service or MDM Service Provider proposed IPS Service and other security monitoring capabilities.
13. Disclose definition of chronic performance issues and current remediation processes.

14. Disclose all applicable national and international industry standards with which this Service will comply.
15. Offer an ongoing, persistent seamless process that is used to monitor network traffic that remains transparent to the Customer minimizing the impact to legitimate traffic Customers.
    a. Initiate a rapid response, as agreed to with the Customer, when legitimate traffic is determined to have been blocked.
16. Ensure that each IPS filter exception submitted includes a detailed history of who (contact information) authorized the exception (Customer must be in approval chain), who submitted the exception, the date that the exception was submitted, and the reasons for the exception.

3.1.3.2 IDS/IPS Log Management and Analysis Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following Log Management and Analysis requirements:

1. Provide automated log monitoring and alert response mechanisms with corresponding actions to resolve.
2. Perform weekly audits of system/device/Application logs and proactively resolve any issues.
3. Collect log-events from device logs, files, directories, databases, and event logs.
4. Transport and centralize the collected log-event data.
5. Convert differing log formats into a common format.
6. Parse additional log formats, as required.
7. Provide a secure encrypted channel to receive log data in a central repository.
8. Store data for a minimum of 30 days, or according to Customer's retention and security requirements.

3.1.4 Host-based Intrusion Prevention Services (HIPS)

MDM Service Provider shall offer Services for configuration, monitoring, change management, and support of HIPS software on endpoint devices including management of endpoint software firewalls. HIPS Services shall include both Customer owned hardware and software and Service Provider owned hardware and software.

3.1.4.1 HIPS Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following HIPS service requirements:

1. Install, update, upgrade, patch, operate, manage, license (as appropriate), administer, and maintain the HIPS, using existing HIPS or MDM Service Provider proposed IPS devices, in accordance with Customer's security requirements for all Software and Equipment in the Customer Environment. Requirement includes upgrades, patches or fixes as needed to Hardware, Software and firmware to ensure optimal performance and capacity of the Service.
2. Install HIPS updates and make configuration changes that address known vulnerabilities or risks to the HIPS as such updates are: identified by the manufacturer of the HIPS; suggested in accordance with industry best practices; or, as required to maintain compliance with Customer security requirements.
3. If a new threat is discovered within Customer's computing environment, write a rule for Customer's written approval to secure Workstations and servers with the host-based firewall functionality.

4. Provide supporting documentation as required to support the Customer's internal and external audit requirements and provide proof of HIPS coverage.
5. Manage, update, and add filters, or blocks, to control unauthorized data sources.
6. Provide recommendations to DIR and Customers on new IPS filters or blocks.
7. Manage automated data exchange capabilities between the IPS Service or MDM Service Provider proposed IPS Service and other security monitoring capabilities.
8. Disclose definition of chronic performance issues and current remediation processes.
9. Disclose all applicable national and international industry standards with which this Service will comply.
10. Monitor for unauthorized access or cyberattacks.
11. Participate in security incident response to provide additional security information the Customer may need to respond to or manage the incident until the threat is mitigated or resolved.

3.1.5 Managed Firewalls

MDM Service Provider shall offer Services for configuration, monitoring, change management, and support of firewall systems at Customer's designated facilities. Managed Firewall Services shall include both Customer owned hardware and software and Service Provider owned hardware and software .

3.1.5.1 Managed Firewall Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following Managed Firewall requirements:

1. Install, update, upgrade, patch, operate and maintain firewall protection Software and Systems in accordance with Customer's security requirements for all Software and Equipment in the Customer Environment.
2. Administer, configure, customize and test out-of-the-box firewall rules for workstations and servers that have been identified, by either the Customer or the MDM Service Provider, as applicable for the firewall security implementation.
3. Continuously tune configurations to maximize firewall capabilities and protections.
4. Create custom firewall rule(s) for Customer's written approval as required by security threats, vulnerabilities, and industry best practices:
   a. If a new threat is discovered within the Customer's computing environment, write a rule for Customer's written approval to secure network infrastructure.
   b. Monitor custom rule deployment and address any of the ad-hoc troubleshooting or maintenance requests in accordance with the established Service Levels.
5. MDM Service Provider must be able to support stateless, stateful, and next-generation firewalls.
6. Monitor for unauthorized access or cyberattacks.
7. Participate in security incident response to provide additional security information the Customer may need to respond to or manage the incident until the threat is mitigated or resolved.
8. Provide two levels of service options, Platinum and Gold, for Customers to select based on availability and mean time to repair service levels defined in **Exhibit 3A** and **Exhibit 3B**.

3.1.6 Web Application Firewalls (WAF)

MDM Service Provider shall offer Services for configuration, monitoring, change management, and support of WAF's. WAF Services shall include both Customer owned hardware and software and Service Provider owned hardware and software.

3.1.6.1 WAF Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following WAF requirements:

1. Install, update, upgrade, patch, operate, and maintain the WAF in accordance with Customer's security requirements for all Software and Equipment in the Customer Environment.
2. Install WAF updates and make configuration changes that address known vulnerabilities or risks to the Web Application Server in accordance with industry best practices, or as required to maintain compliance with Customer security requirements.
3. Continuously tune configurations to maximize firewall capabilities and protections.
4. If a new threat is discovered within Customer's computing environment, write a rule for Customer's written approval to secure the protected web application.
5. Provide written documentation of WAF coverage, as required by the Customer.
6. Respond to and confirm any suspected high events and make recommendations on whether traffic is malicious or legitimate and whether or not mitigations should be put into effect.
7. Monitor for unauthorized access or cyberattacks.
8. Participate in security incident response to provide additional security information the Customer may need to respond to or manage the incident until the threat is mitigated or resolved.

3.1.7 Security Information and Event Management (SIEM)

MDM Service Provider will offer SIEM Services as a managed or hosted solution that provides real-time analysis of security alerts generated by systems and applications.

3.1.7.1 SIEM Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following SIEM requirements:

1. Install, configure, and manage hardware and software required for the purposes of event transmission, collection, correlation, and reporting in SIEM and log management systems in accordance with Customer policy.
2. Provide SIEM service and propose associated backup strategy and tools for any eligible Customers that may require them.
3. Support Network Time Protocol (NTP).
4. SIEM Services shall be provided in a high availability architecture.
5. Employ appropriate methods to ensure that service outages to the SIEM solution do not result in a loss of event data in the collection or storage processes.
6. Develop the patching strategy in coordination with the Customer.
7. Develop and maintain an inventory of Customer's systems and applications with all alerts being collected and analyzed. The service and system inventory shall include at a minimum: application names; service names; versions; service descriptions;

data collection method; data collection component; and, event description documentation.

8. Make inventory information available to Customer's authorized personnel as required and for auditing purposes.
9. Retain all collected SIEM data and logs in accordance with the Customer's applicable data retention requirements.
    a. The minimum data and log retention period for this service shall be 30 calendar days for both online and archive storage and shall be included in the MDM Service Provider's pricing for this service.
    b. Customers requesting to obtain additional storage may purchase that storage from the MDM Service Provider as a pass-through expense as defined in **Exhibit 4.**
10. Participate in the security incident response processes to provide necessary resources to support resolving security incidents.
11. Perform regular SIEM and log management system and component performance assessments and tuning exercises.
12. Establish a process to proactively monitor key SIEM components' performance.
13. Establish mechanisms so that SIEM content will trigger specified alerts.
14. Provide for a private network connection to Customer for the purposes of reporting on requested content.
15. Provide mechanisms so that any real-time alarms, reports and email notifications may be directed at more than one Customer user. Designated recipients may be individual Customer security agents or a larger distribution list. Customer must be able to make custom designations of recipients for custom content.
16. Provide custom content development, custom content tuning, real time alarming, escalation to Customer, and proactive content development in response to public and private threats.
17. Equipment which requires monitoring may include, but are not limited to security, network, and endpoint devices or applications.
18. Ensure that the SIEM solution is capable to produce the following types of content:
    a. Customizable real-time rules, based on complex logic.
    b. Customizable, scheduled and ad-hoc reporting based on complex queries with complex logic.
    c. Customizable page and content layout.
    d. Trending data based on source log values. Trending will be used in both reporting and proactive anomaly detection and alerting.
    e. Data values that result from custom real-time rules used for future reporting or secondary rules.
    f. Filter logic will be applied to existing rules, reports, and event feeds sent to the SIEM for capacity management.
19. Normalize log values for all supported log feeds into a common set of fields for all feeds. The normalization and uniform nature of fields is the essential core of an effective SIEM. Log feeds must have at a minimum, common fields for:
    a. Source and destination IP address and port
    b. Source and destination username
    c. Original device IP address and username
    d. Original process and Application
    e. Original Application identification
    f. Original event name
20. Provide a secure encrypted channel to receive log data into a central repository.

21. Provide designated Customer users full read-only access to real-time and historical event feeds, rule logic, report components, filters, data lists, variables, queries for validation and investigation.
22. Provide Customer authorized users with the ability to develop and apply complex read-only query logic to real-time and historical data.
23. Accept threat alert notifications from Customer via agreed upon input method(s) and apply logic to determine appropriate response to threat. Implement appropriate response to threat in accordance with established Customer protocols.
24. Provide on-call after hour monitoring and notification to Customer in accordance with Service Management Manual process.
25. Monitor for unauthorized access or cyberattacks.
26. Implement agreed upon response protocols based on agreed upon Customer-defined thresholds during standard hours and after hours.
27. Provide support for Distributed Denial of Service (DDOS) attacks in accordance with agreed upon protocols and monitoring levels.

3.1.7.2 SIEM Log Management and Analysis Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following Log Management and Analysis requirements:

1. Provide automated log monitoring and alert response mechanisms with corresponding actions to resolve.
2. Perform weekly audits of system/device/Application logs and proactively resolve any issues.
3. Collect log-events from device logs, files, directories, databases, and event logs.
4. Transport and centralize the collected log-event data.
5. Convert differing log formats into a common format.
6. Parse additional log formats, as required.
7. Provide a secure encrypted channel to receive log data in a central repository.
8. Store data for a minimum of 30 days, or according to Customer's retention and security requirements.

3.1.8 Targeted Threat Research

MDM Service Provider will develop plans to correlate information targeted to a Customer's environment with knowledge of extant threats to assist in structuring pro-active response to credible threats. Targeted Threat Research is in addition to any threat research required to perform other Services in this statement of work.

3.1.8.1 Targeted Threat Research Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following Threat Research requirements:

1. Make use of multiple sources of information to develop confidence in threat environment.
2. Develop a profile of extant threats targeted to the Customer environment.
   a. Gather and correlate threat data from multiple sources including device logs, security devices, SIEM systems, etc., to develop a catalog of potential threats.
   b. Obtain advance warning of impending attacks against shared IT infrastructure (for example, the global Domain Name System), infrastructure controlled by customer IT organizations, or online services provided to customers and partners.

   c. Identify potential resources, tools, and techniques that could be used to prevent the exploitation of the identified threats.
   d. Based on potential threats, resources, tools, and techniques, catalog a subset of credible threats.
3. Gather information regarding susceptibility of the Customer's environment to credible threats.
   a. Identify vulnerabilities in the Customer's environment from sources including vulnerability scans.
   b. Estimate the potential target desirability of Customer's information assets and the impact if those Customer's information assets are compromised.
   c. Based on credible threats, vulnerabilities, and value, catalog a subset of high-priority threats.
4. Identify recommended mitigation measures to counter high-priority threats.
   a. Recover compromised authentication credentials
   b. Leverage real-time operational support for responses to security events (for example, takedown of phishing sites, forensic support, or analysis of malware or other artifacts).Provide analysis of enterprise trends and significant security events that impact Customer's environment.
   a. Develop case studies for use in internal incident response training exercises and business continuity management efforts.
   b. Gather information about emerging malware and other malicious-code threats.
   c. Prioritize vulnerability management activities based on risk criteria that include the likelihood of a given threat materializing
   d. Monitor changes to the external environment to define triggering events that will require infrastructure refresh.

3.1.9 Malware Detection System/Malware Prevention System Device Management (MDS/MPS)

The MDM Service Provider shall meet or exceed the following MDS/MPS requirements. MDM Service Provider shall offer Services for configuration, monitoring, change management, and support of the Customer's MDS/MPS. MDS/MPS Services shall include hardware and software owned by the Customer, third-party, and/or MDM Service Provider. The platform will analyze events for signs of possible security events/incidents, including, but not limited to, violations or imminent threats of violation of computer security policies, acceptable-use policies, malware propagation or security best practices. This Service shall include automated responses to detected security events/incidents, including, but not limited to, dropping packets, resetting connections, generating alerts, or quarantining intruders

3.1.9.1 MDS Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following MDS service requirements:

1. Install, update, upgrade, patch, operate, manage, license (as appropriate), administer, and maintain network malware detection and prevention systems for all networks specified by Customer, using existing MDS/MPS or MDM Service Provider provided MDS/MPS devices, in accordance with Customer's security requirements for all Software and Equipment in the Customer Environment. Requirement includes upgrades, patches, or fixes as needed to Hardware, Software, and firmware to ensure optimal performance and capacity of the Service

2. Configure the network-based MDS/MPS so as to comply with Customer's security requirements in order to identify, monitor, and potentially block suspicious patterns that may indicate abnormal activity or intrusion attempts. MDM Service Provider shall notify the Customer of high risk events as applicable.
3. Continuously tune configurations to maximize firewall capabilities and protections.
4. Monitor the Customer Networks for external intrusions and cyber-attacks and alert the appropriate Customer personnel so that countermeasures may be taken.
5. Perform ongoing tuning of the network MDS/MPS, system signatures, and configuration settings to minimize invalid alerts (i.e., false positives, alert volume, incorrectly blocked traffic, nuisance alerts, etc.). Such tuning must be authorized by Customer and documented by the MDM Service Provider as required by the Customer.
6. Upgrade the network MDS/MPS and all associated rules, signatures, settings and software when upgrades are: provided by the applicable manufacturer; when such upgrades are in accordance with industry best practices; or, as required to maintain compliance with Customer's security requirements.
7. Retain all collected data and logs in accordance with the Customer's applicable data retention requirements.
    a. The minimum data and log retention period for this service shall be 30 calendar days for both online and archive storage and shall be included in the MDM Service Provider's pricing for this service.
    b. Customers requesting to obtain additional storage may purchase that storage from the MDM Service Provider as a pass-through expense as defined in **Exhibit 4**, Pricing and Financial Revisions, Section 10, Pass-Through Expenses.
8. Participate in security incident response to provide additional security information the Customer may need to respond to or manage the incident until the threat is mitigated or resolved.
9. Manage, update, and add filters, or blocks, to control unauthorized data sources.
10. Provide recommendations to DIR and Customers on new MDS/MPS filters or blocks.
11. Manage automated data exchange capabilities between the MDS/MPS Service or MDM Service Provider proposed MDS/MPS Service and other security monitoring capabilities.
12. Disclose definition of chronic performance issues and current remediation processes.
13. Disclose all applicable national and international industry standards with which this Service will comply.
14. Offer an ongoing, persistent seamless process that is used to monitor network traffic that remains transparent to the Customer minimizing the impact to legitimate traffic Customers.
    a. Initiate a rapid response, as agreed to with the Customer, when legitimate traffic is determined to have been blocked.
15. Ensure that each MDS/MPS filter exception submitted includes a detailed history of who (contact information) authorized the exception (Customer must be in approval chain), who submitted the exception, the date that the exception was submitted, and the reasons for the exception.

3.1.9.2 MDS/MPS Log Management and Analysis Service Requirements

At a minimum, the MDM Service Provider shall meet or exceed the following Log Management and Analysis requirements:

1. Provide automated log monitoring and alert response mechanisms with corresponding actions to resolve.
2. Perform weekly audits of system/device/Application logs and proactively resolve any issues.
3. Collect log-events from device logs, files, directories, databases, and event logs.
4. Transport and centralize the collected log-event data.
5. Convert differing log formats into a common format.
6. Parse additional log formats, as required.
7. Provide a secure encrypted channel to receive log data in a central repository.
8. Store data for a minimum of 30 days, or according to Customer's retention and security requirements.

3.1.10 Security Operations Center (SOC) Services

Some Customers maintain a Security Operations Center (SOC) providing managed security services to multiple customers. The requirements below define Services that the Service Provider shall provide to Customers.

3.1.10.1 SOC Monitoring and Alerting Requirements

SOC monitoring and alerting is a key service that is provided to the Customer. The SOC monitoring and alerting Services are network traffic, tool based alerts and packet based analysis. E.g., there are 2.8 million plus public IPs that the DIR SOC provides internet services to with over 100+ diverse customers and therefore is set up more like an Internet Service Provider (ISP). The MDM Service Provider shall perform the following SOC Monitoring and Alerting Requirements at a minimum:

1. Provide Network Security Monitoring, Alerting and Analysis Services that monitors the Customer's networks for external intrusions and cyberattacks and alerts the proper State authorities so that countermeasures may be taken.
2. Monitor and alert using existing customer-provided tools (IPS, multiple IDS, Network Forensic Tool, Malware Detection System, and other Customer provided tools) at the Customer's SOC facility. Service Provider shall vet all Indicators of Compromise and alerts to determine if any customer alerts or proactive blocks are required to be put in place on Customer's firewall and/or IPS.
3. Alert Customers and implement proactive blocks as necessary.
4. Incorporate threat intelligence received either via email or an alert from a security tool. Service Provider shall vet these Indicators of Compromise to determine if the Service Provider should send any alerts or place proactive blocks on the Customer's IPS and/or firewall.
5. Vet alerts to determine whether the alert should be sent to one or more of the Customers. Service Provider shall send alerts via email and then loaded into GRC Archer the statewide incident tracking system. Service Provider shall maintain updated, accurate contact lists for all Customers.
6. Vet each alert to ensure true positive rate for alerts sent to Customers. The Service Provider shall attempt to maintain an expected target of 95% true positive rate with a minimum of 90%.
7. Provide Customers with, at a minimum, two (2) Proof of Concepts (POCs) annually to evaluate new and emerging technologies. These POCs can either be a comparison of different vendors who offer similar technologies or as an exploratory evaluation of a new unique technology. These POCs are performed to address an identified gap in the SOC security program or to determine if a technology fits well in the environment. Service Provider may propose POCs or the Customer may request

a POC. Service Provider shall consult with each Customer on any proposed POC and schedule to determine viability of conducting the POC. The vendor shall generate a comprehensive evaluation report using a Customer approved template that summarizes the findings.

8. Respond to and confirm any suspected high events and make recommendations on whether traffic is malicious or legitimate and whether or not mitigations should be put into effect while working with the Customer's ISP DDOS monitoring service.
9. Provide malware detection Services for Customer Security Operations Centers. Customers may have Malware detection and sandboxing through a next gen Firewall and/or through endpoint protection and detection services.
10. Provide analysis during contracted working hours, with on call resources to respond to alerts on off hours. True positives require the Service Provider to either put a block in place to stop communication to and from the infected host or send an alert to the appropriate customer.
11. Triage and vet alerts using DIR's Network Forensic Tool with staff located onsite at the DIR SOC. Service Provider may perform after hours monitoring offsite at Service Provider locations. Service Provider shall provide staff on call to respond to critical events that may arise after hours.

3.1.10.2 SOC Monitoring and Alerting Requirements Remote 24x7

The Service Provider shall provide Remote 24x7 services in compliance with requirements in Section 3.1.10.1 (SOC Monitoring and Alerting Requirements) above with modifications to the requirements of #2 and #11, as reflected below:

2. Remotely monitor and alert up to a maximum of fifteen customer provided tools, including but not limited to: Trend Micro IPS, FireEye MDS, RSA NetWitness Packet Analyzer, Security Onion Snort IDS, Security Onion Bro Log Analyzer, DDoS Alerts from circuit providers, and alerts from other managed alerting services. Service Provider shall investigate all indicators of compromise and alerts to determine if any Customer alerts or proactive blocks are required to be put in place on Customer's firewall and/or IPS.

11. Triage and vet alerts using DIR's Network Forensic Tool with remote staff located offsite. Service Provider will also perform after hours monitoring offsite at Service Provider locations. Service Provider shall provide staff on call to respond to critical events that may arise after hours.

In addition, the Service Provider shall provide the following Remote 24x7 SOC Monitoring and Alerting Requirements :

1. Provide remote operational management during the core hours of 6AM-6PM Monday-Friday, to include the following:
   a. (1) Dedicated Operations Manager, (3) Dedicated SOC Tier III personnel functioning in the roles of SOC Analyst and Engineer.
   b. Perform operational changes to monitored devices in support of security operations, effecting system functionality, system configuration and settings.
   c. Help direct and coordinated business unit responses with MSS based services.

   Provide remote SOC monitoring, alerting, and support for identified customer environments and systems. Provide monitoring and alerting service support during noncore hours 5 PM-7 AM Monday-Friday, 24/7 coverage Saturday and Sunday and Holidays.

Service Provider will leverage Tier II and Tier III remote resources for noncore hour weekday shifts (5PM-7AM Monday-Friday), 24/7 Saturday and Sunday and holiday coverage.

2. Provide Security Information and Event Management (SIEM) in compliance with requirements in Section 3.1.6 of this document for up to a maximum of fifteen customer owned hardware and software devices.

3.1.10.3 SOC Monitoring and Alerting Requirements 24x7

In addition to the SOC monitoring and alerting requirements in Section 3.1.10.1 (SOC Monitoring and Alerting Requirements) above, this service includes program and device management, vulnerability scanning, and SOC 24x7 active monitoring.

The Service Provider shall provide the following 24x7 SOC Monitoring and Alerting Requirements:

1. Provide onsite program management during the hours of 8AM-5PM Monday-Friday, to include the following:
   a. Senior level oversight of all services delivered to Customer
   b. Coordination among one or more Customer business units, when applicable;
   c. Communication associated with the services provided, to include tracking and reporting as needed, and representation as needed by Customer leadership.

   Service Provider will leverage Tier II remote resources for 2nd and 3rd shift weekday shifts (5PM-8AM Monday-Friday), weekend shifts, and holiday coverage. Tier III support will be provided through an on-call process, where Tier II will contact Tier III in the event of an escalation.

2. Provide up to three device management services in compliance with below specific requirements for customer owned hardware and software only:
   a. Endpoint Device Management, per Section 3.1.1 of this document.
   b. Intrusion Detection Services / Intrusion Prevention Services (IDS/IPS), per Section 3.1.2 of this document.
   c. Host-Based Intrusion Prevention System (HIPS), per Section 3.1.3 of this document.
   d. Managed Firewalls, per Section 3.1.4 of this document.
   e. Web Application Firewalls (WAF), per Section 3.1.5 of this document.
   f. Security Information and Event Management (SIEM), per Section 3.1.6 of this document.
   g. Targeted Threat Research, per Section 3.1.7 of this document
   h. Malware Detection System / Malware Prevention System Device Management (MDS/MPS), per Section 3.1.8 of this document

3. Provide risk and compliance service in compliance with below specific requirements for customer owned hardware and software only:
   a. Vulnerability Scanning, per Section 3.1.4 of Exhibit 2.8.3.

3.1.10.4 DIR SOC Specifications

DIR's Security Operations, described in Appendix D, is an example of an MSS Customer that will purchase the SOC Services.

DIR's SOC employs a Network Forensics Tool (NFT) that DIR owns and currently stores 10+ days of full packet capture and 6 weeks of metadata for all internet traffic coming into and out of the network that DIR manages. DIR has a series of IDS's and MDS's that it owns and these tools generate tool based alerts that are used as potential indicators of compromise (IOC's) for infected machines or ongoing cyber-attacks. DIR also has IDS monitoring Services established with the Multi State Information Sharing and Analysis Center (MS-ISAC, a division of the Department of Homeland Security) and the University of Texas at Austin to provide additional SOC security analyst eyes into our network traffic events for any suspicious or anomalous traffic.

Malware Detection services are provided at the DIR SOC location using DIR owned hardware and software. The DIR SOC utilizes a network based malware detection system or (MDS). This MDS analyzes traffic that is permitted to pass through DIR's internet gateways and then detonates any suspicious or malicious traffic in a virtual sandbox with multiple virtual Operating Systems to determine if any malware attachments are being sent or received. This analysis is also conducted to determine if malware is being delivered to customer assets and conversely if a customer asset is beaconing out or infected with any known malware. DIR owns its MDS system. The Service Provider shall analyze outputs or alerts from the tool and determine what, if any, are false positives and which are true positives.

3.1.11 Advanced Threat Hunting

This section identifies requirements for Advanced Threat Hunting. Advanced Threat Hunting provides monitoring of customer environments for potentially suspicious or unwanted software stored or running on the device via automated tools. This service may be via a one-time scan or a subscription in which continuous monitoring is performed for a specified period of time.

3.1.11.1 Advanced Threat Hunting One-Time Scan Requirements

The intent of Advanced Threat Hunting One-Time Scan is to conduct a one-time forensics analysis of the customer environment using advanced threat hunting techniques. The Service Provider shall perform the following Advanced Threat Hunting One-Time Scan requirements, unless otherwise determined by DIR or DIR Customer and agreed by Service Provider:

1. Install, update, upgrade, patch, operate, manage, license (as appropriate), administer, and maintain ATH Controller system(s) used to scan all devices specified by Customer, using the existing Service Provider provided ATH systems (hardware and software), in accordance with Customer's security requirements for all systems supporting services delivered in the Customer environment. Requirement includes upgrades, patches, or fixes as needed to hardware, software, and firmware to ensure optimal performance and capacity of the Service.
2. Configure the ATH system to comply with Customer's security requirements in order to identify, monitor, and notify on suspicious patterns that may indicate abnormal activity, intrusion attempts or other indicators of compromise. Service Provider shall notify the Customer of high-risk events as applicable.
3. Continuously tune configurations to maximize ATH capabilities and protections.

4. Monitor the Customer specified devices for the presence of malware and persistent threats and alert the appropriate Customer personnel so that countermeasures may be taken.
5. Perform tuning of the ATH system signatures, and configuration settings to minimize invalid alerts (i.e., false positives, alert volume, incorrectly blocked traffic, nuisance alerts, etc.).
6. Make use of information developed from other MSS services and/or stored in the Data Repository to enhance the configuration and effectiveness of the ATH service.
7. Participate in security incident response to provide additional security information the Customer may need to respond to or manage the incident until the threat is mitigated or resolved.
8. Provide recommendations to DIR and Customers on new ATH filters or rules.
9. Disclose definition of chronic performance issues and current remediation processes.

3.1.11.2 Advanced Threat Hunting Subscription Requirements

The intent of Advanced Threat Hunting Subscription is to perform a continuous forensics analysis of the customer environment using advanced threat hunting techniques. The Service Provider shall perform the following Advanced Threat Hunting (ATH) Subscription requirements, unless otherwise determined by DIR or DIR Customer and agreed by Service Provider:

1. Install, update, upgrade, patch, operate, manage, license (as appropriate), administer, and maintain ATH systems for all devices specified by Customer, using the existing Service Provider provided ATH systems (hardware and software), in accordance with Customer’s security requirements for all systems supporting services delivered in the Customer environment. Requirement includes upgrades, patches, or fixes as needed to hardware, software, and firmware to ensure optimal performance and capacity of the Service.
2. Configure the ATH system to comply with Customer’s security requirements in order to identify, monitor, and notify on suspicious patterns that may indicate abnormal activity, intrusion attempts or other indicators of compromise. Service Provider shall notify the Customer of high-risk events as applicable.
3. Continuously tune configurations to maximize ATH capabilities and protections.
4. Monitor the Customer specified devices for the presence of malware and persistent threats and alert the appropriate Customer personnel so that countermeasures may be taken.
5. Perform ongoing tuning of the ATH system signatures, and configuration settings to minimize invalid alerts (e.g., false positives, alert volume, incorrectly blocked traffic, nuisance alerts, or others). Such tuning must be authorized by Customer and documented by the Service Provider as required by the Customer.
6. Upgrade the ATH and all associated rules, signatures, settings, and software when upgrades are provided by the applicable manufacturer; when such upgrades are in accordance with industry best practices; or, as required to maintain compliance with Customer’s security requirements.
7. Make use of information developed from other MSS services and/or stored in the Data Repository to enhance the configuration and effectiveness of the ATH service.
8. Collect event logs from monitored devices and securely transport the collected log-event data to the SIEM.

9. Retain all collected data and logs in accordance with the Customer's applicable data retention requirements.
    a. The minimum data and log retention period for this service shall be 30 calendar days for both online and archive storage.
    b. Customers requesting to obtain additional storage may purchase that storage from the Service Provider as a pass-through expense as defined in Exhibit 4, Pricing and Financial Revisions, Section 10, Pass-Through Expenses.
10. Participate in security incident response to provide additional security information the Customer may need to respond to or manage the incident until the threat is mitigated or resolved.
11. Provide recommendations to DIR and Customers on new ATH filters or rules.
12. Manage automated data exchange capabilities between the ATH Service and other security monitoring capabilities (primarily the SIEM).
13. Disclose definition of chronic performance issues and current remediation processes.